KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Before the Federal Trade Commission
Dot Com Disclosures, P114506
Comments of the Center for Democracy & Technology

August 10, 2011

The Center for Democracy & Technology (CDT) appreciates the opportunity to respond to the questions posed by the Commission as it considers updating and reissuing its Dot Com Disclosures. Since 2000, technological innovations have greatly altered the internet landscape and CDT applauds the Commission for undertaking a review of its Dot Com Disclosures. The past eleven years have seen fundamental shifts in the way individual ads are deployed and even in the functions they serve. These shifts call for greater transparency from advertisers about not only the messages that each advertisement conveys, but also other facets of each ad: for example, the data collection that occurs "behind the scenes" as an ad is being served or the fact that the ad is being targeted at a viewer on the basis of her past activities.

In these comments, we focus on three types of activities that we believe necessitate greater transparency from the advertising industry and businesses engaged in related practices[1]: data collection and use as it relates to online behavioral advertising; data collection and use as it relates to the Digital Out-Of-Home industry and the burgeoning Internet of Things; and multi-party selling arrangements known as online subscription upselling.

[1] Transparency alone is insufficient to protect consumer privacy – any comprehensive privacy regime requires implementation of a full set of Fair Information Practice principles (FIPs). However, given the context of this consultation, we have limited our discussion in these comments to the need for greater transparency around certain data collection and use practices. CDT has written at considerable length about the key role of FIPs as guideposts for any consumer privacy framework. *See e.g.,* Center for Democracy & Technology, *Refocusing the FTC's Role in Privacy Protection: Comments of the Center for Democracy & Technology In regards to the FTC Consumer Privacy Roundtable* (November 2009), *available at* http://www.cdt.org/files/pdfs/20091105_ftc_priv_comments.pdf; Center for Democracy & Technology, *Comments of the Center for Democracy & Technology in the Matter of A National Broadband Plan for our Future - NBP Public Notice #29* (January 2010), *available at* http://www.cdt.org/files/pdfs/20100125_cdt-fcc_comments.pdf.

What issues have been raised by online technologies or Internet activities or features that have emerged since the business guide was issued that should be addressed in a revised guidance document?

In 2000, the typical Internet-based advertisement did little more than display, via a website, information relevant to a product or service. Today, Internet-based advertisements have expanded to new mediums – mobile apps, digital signage, and even television sets – and new functions for these ads have emerged. These new mediums and new functions present challenges for transparency that we urge the Commission to address through its updated Dot Com Disclosure guidelines.

Data Collection by web-based and app-based advertisements

Traditionally, advertisements served a single purpose: they communicated a message to consumers. Today, many web-based and app-based advertisements serve an additional purpose: they collect detailed information about each consumer who views the advertisement. Code embedded in advertisements and websites allows advertising networks to collect large quantities of information about website visitors and their activities across the web. Using a variety of technologies and techniques,[2] this data may then be linked to information about the consumer's web-browsing history,[3] purchase history,[4] political leanings,[5] home-buying data,[6] income,[7] social network profiles,[8] or even to her name and email address.[9] In an in-depth series on online data collection published recently by the *Wall Street Journal*, the paper presented examples of advertising networks that, through such data collection, had correctly identified individual users' ages, health and wellness goals, income, hometown, education levels, interests, and favorite movies.[10]

---

[2]See footnotes 3-12 below.

[3]Julia Angwin, The Web's New Gold Mine: Your Secrets, THE WALL STREET JOURNAL, July 30, 2010, http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

[4]Emily Steel and Julia Angwin, The Web's Cutting Edge, Anonymity in Name Only, THE WALL STREET JOURNAL, August 4, 2010, http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html.

[5]See, e.g., Emily Steel, A Web Pioneer Profiles Users by Name, THE WALL STREET JOURNAL, October 25, 2010,

http://online.wsj.com/article/SB10001424052702304410504575560243259416072.html.

[6]Emily Steel and Julia Angwin, The Web's Cutting Edge, Anonymity in Name Only, THE WALL STREET JOURNAL, August 4, 2010, http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html.

[7]*Id.*

[8]Emily Steel, A Web Pioneer Profiles Users by Name, THE WALL STREET JOURNAL, October 25, 2010, http://online.wsj.com/article/SB10001424052702304410504575560243259416072.html.

[9]*Id.*

[10]Julia Angwin, The Web's New Gold Mine: Your Secrets, THE WALL STREET JOURNAL, July 30, 2010, http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html; Emily Steel and Julia Angwin, The Web's Cutting Edge, Anonymity in Name Only, THE WALL STREET JOURNAL, August 4, 2010, http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html.

Extensive studies and reports have also demonstrated that it is becoming increasingly difficult for users to exercise control over the collection of the data that yields these inferences: in response to a growing population of users who remove cookies and take other "good housekeeping" measures for the express purpose of preventing tracking, many companies have devised new means for tracking users, some of which are impossible for users to block.[11] As browsers and web standards continue to evolve, offering new capabilities such as offline data storage and new APIs for interactive web applications, so do the exploits developed to thwart consumers' choices.[12] Meanwhile, consumer tracking methods, first created for the PC, have also been adopted by advertising networks in the mobile space, where even more sensitive information – such as precise location data – is up for grabs.[13]

Yet studies have consistently found that consumers do not understand that ads serve this dual purpose nor, upon learning how code embedded in advertisements is used to collect data about them, are they comfortable with this practice.[14] They certainly do not understand that simply by viewing an ad they are "consenting" to be tracked across the web, and potentially offline as well.[15]

In short, these studies demonstrate that just as a false or otherwise deceptive advertising claims violate the typical consumer's sense of fairness, the data collection activities that occur through advertisements and web bugs violate the typical consumer's expectation of privacy. And just as the Commission's original Dot Com Disclosure guidelines clarified that false or otherwise deceptive advertising claims that are not tolerated in print would not be tolerated online and that companies should transparently qualify their messages, the Commission's updated guidelines should clarify that certain online data collection practices are considered deceptive and that participating companies should transparently explain their practices.

---

[11] Julia Angwin and Jennifer Valention-Devries, Race is on to Fingerprint Phones, PCs, THE WALL STREET JOURNAL, November 30, 2010, http://online.wsj.com/article/SB10001424052748704679204575646704100959546.html; Ryan Singel, Researchers Expose Cunning Online Tracking Service That Can't Be Dodged, WIRED, July 29, 2010, http://www.wired.com/epicenter/2011/07/undeletable-cookie/.

[12] *See e.g.,* Mika Ayenson et al. *Flash Cookies and Privacy II, Now With HTML5 and ETag Respawning*, July 29, 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390; Ryan Singel, Researchers Expose Cunning Online Tracking Service That Can't Be Dodged, WIRED, July 29, 2010, http://www.wired.com/epicenter/2011/07/undeletable-cookie/; Jonathan Mayer, *Tracking the Trackers: To Catch a History Thief*, July 19, 2011, http://cyberlaw.stanford.edu/node/6695.

[13] *See e.g.,* Julia Angwin and Simon Constable, Video: How Smartphone Apps Spy on You, THE WALL STREET JOURNAL, December 17, 2010, http://online.wsj.com/video/how-smartphone-apps-spy-on-you/A0E0DF80-9235-4DAC-9206-1E9D25354A55.html; Jennifer Valentino-Devries and Julia Angwin, Latest Treasure is Location Data, THE WALL STREET JOURNAL, May 10, 2011, http://online.wsj.com/article/SB10001424052748703730804576313522337383898.html.

[14] A 2009 study conducted by researchers at UC Berkeley and the University of Pennsylvania's Annenberg School of Communication found that, if given a choice, 68% of Americans "definitely would not" allow advertisers to follow them online even if their online activities would remain anonymous. Nineteen percent "probably" would not allow this tracking. Sixty-three percent of Americans feel that laws should require advertisers to delete information about their Internet activity immediately. Joseph Turow, Jennifer King, Chris Hoofnagle, Amy Bleakly & Michael Hennessy, Contrary to What Marketers Say, Americans Reject Tailored Advertising and Three Activities that Enable It, Pg. 3 (Sep. 29, 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[15] *Id.*

Data use

In addition to expressing concern over the data collection that is often associated with the display of advertisements or the loading of websites, consumers have also expressed concern over the targeted nature of what are known as behavioral advertisements.[16] Behavioral ads are selected for individual consumers based not on the context of the website they are visiting or the app they are using, but based on other information about their activities: past web browsing behavior, past purchase behavior, demographic information, etc. For example, a consumer who has recently been researching environmentally friendly cars might be reading an article about a summer blockbuster and see an ad for a hybrid.

Indeed, data use is the area where we have seen the most transparency from members of the online advertising ecosystem. Most recently, the Digital Advertising Alliance has begun implementing common iconography into online ads that allow consumers to access information about the sources of information behind those ads.[17] However, this process was only instigated following continued pressure from the Commission and has not been adopted for ads shown on the mobile web or via mobile apps. All in-ad notices allow users to opt out of receiving targeted advertisements; they do not, however, always allow users to opt out of being tracked as they browse the web.[18]

Transparency

CDT urges the Commission to clarify in its guidelines that behaviorally-targeted ads should display such consumer notice like the Digital Advertising Alliance's iconography. This notice requirement should extend to sites where behaviorally-targeted advertisements are not shown but third-party data collection is nonetheless occurring. The concept of in-ad notice should also extend to mobile ads. Such icons should be placed in a sensible location and displayed at a time relevant to user's decision to opt in or opt out of data collection and use. Icons should link to notices that are easy for the average person to understand, are presented in a few short sentences. Notices should, however, disclose both the purposes of data collection and whether that data will then be transferred to other parties. Finally, the Commission should find that all notices link to a meaningful opt out mechanism, one that allows consumers to opt out of third-party data collection as well as relevant data uses.

However, some special and sensitive categories of data should be used only *after* receiving a user's affirmative, opt-in consent. Often, advertising networks reach conclusions that implicate sensitive health concerns: based on users' web browsing activities, some ad networks utilize "interest-based" categories such as cholesterol management, blood sugar management, weight loss, smoking cessation, and arthritis.[19] CDT firmly believes that companies should only use sensitive consumer information – such as health or sexuality related information – for marketing

---

[16] A 2009 study conducted by researchers at UC Berkeley and the University of Pennsylvania's Annenberg School of Communication found that between eighty and ninety percent of adults of all ages reject advertisements that are tailored based on their activities across multiple Web sites. *Id.*

[17] *See* The Digital Advertising Alliance, *The Self-Regulatory Program for Online Behavioral Advertising*, http://www.aboutads.info/ (Last visited August 7, 2011).

[18] *See* Jonathan Mayer, *Tracking the Trackers: Early Results*, Blog Post, July 12, 2011, http://cyberlaw.stanford.edu/node/6694.

[19] *See* Yahoo!, *Yahoo Privacy: All Standard Categories,* http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/asc/details.html (Last visited August 7, 2011).

after receiving the consumer's affirmative consent after clear and conspicuous disclosure from the company. This position is consistent with what the Commission previously advocated in its 2009 Self-Regulatory Principles for Online Behavioral Advertising, where it stated that "companies should only collect sensitive data for behavioral advertising after they obtain affirmative express consent from the consumer to receive the advertising."[20]

Obtaining meaningful consent must be carefully implemented across both functional and aesthetic contexts. There is no "one size fits all" solution. Appropriate consent mechanisms must be designed with particular products and services in mind. Finally, while many argue that the smaller screen size on mobile devices is an impediment to notice the opposite is in fact true: with less clutter, smaller screens often make it easier – not more difficult – to convey clear notice to consumers.

What issues raised by new technologies or Internet activities or features on the horizon should be addressed in a revised business guide?

A number of new technologies have especially concerning implications for privacy. Consider for example the Digital Out-Of-Home (DOOH) industry, which produces digital signage or "smart signs," a communications medium characterized by a dynamic display that presents messages in a public environment. The DOOH industry is currently exploring several technologies that will improve audience measurement and interactivity. Depending on the system, these enhancements often obtain a range of information about consumers. Some of the technologies, such as facial recognition, RFID, and license-plate scanning technologies, have the ability to identify individual consumers, track them as they move from place to place and store detailed information about their preferences and activities.[21]

Using identification and interactivity technologies, the DOOH and mobile industries are taking the Internet experience into the physical world. In doing so, DOOH has established a burgeoning offline version of the behavioral advertising that currently occurs online – the practice of tracking consumers' activities in order to deliver advertising targeted to the individual interests.

Consumers and companies are already wary of the privacy implications of identification and consumer profiling technologies in DOOH. Comments to blog posts and news articles on facial recognition in digital signage indicate many consumers have little faith that DOOH companies will protect consumer data.[22] Some industry figures have indicated that success will require that

[20] Federal Trade Commission, FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising, Pg. 2 (Feb. 2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[21] For more information about these techniques and the privacy implications of DOOH, *see* Center for Democracy & Technology, *Building the Digital Out-Of-Home Privacy Infrastructure* (March 1, 2010), http://www.cdt.org/files/pdfs/Building%20the%20Digital%20Out-Of-Home%20Privacy%20Infrastructure_0.pdf.

[22] Nilay Patel, TruMedia says its facial-recognition bilboards will never record video, it won't share with cops – User Comments, Engadget, June 10, 2008, http://engadget.com/2008/06/10/trumedia-says-its-facial-recognition-billboards-will-neverrecor/#comments.

companies must guarantee consumer privacy,[23] while others have cited privacy issues as an obstacle to using facial recognition technology for advertising purposes.[24] A *New York Times* article on billboards with facial recognition prompted a major DOOH company to publicly defend its privacy practices.[25] Public backlash and possible violations of existing privacy laws have already led to the discontinuation of some DOOH advertising projects, as with the billboard which scanned UK license plates.

Privacy standards for DOOH, as for other technologies, should be based on all of the widely accepted Fair Information Practice Principles (FIPPs). Through its updated Dot Com Disclosure guidelines, the Commission should build on guidelines already published by the Digital Signage Federation and work to ensure that members of the DOOH industry specifically incorporate the transparency principle into the deployment of their data collection technologies and advertisements. [26]

At present, most DOOH companies are completely unknown to consumers, so consumers are unlikely to look for the privacy policies posted on the websites of DOOH companies. Even if consumers come to know the names of DOOH companies, current practices give consumers little hint as to what company is responsible for a given DOOH display. The challenge for the Commission is to work with DOOH companies to find a way to present meaningful notice at the point of data collection. Such notice is fundamental to transparency. CDT urges the Commission to require that DOOH companies give clear, prominent notice of DOOH media units that collect consumer data at the physical location in which the unit operates. To the extent possible, the notice should appear conspicuously on or close to each DOOH unit that is collecting the information. One notice should not cover, for example, an entire supermarket, but instead should be at each sensor and associated DOOH screen within the supermarket. There should be no hidden receivers, cameras or sensors used exclusively for marketing.

The Commission should further clarify that generic notices like “These premises are under video surveillance” are not sufficient. Consumers have come to assume such notices to relate to security measures, not marketing. Such notices do not provide accurate notification of the more comprehensive data collection, sharing and usage associated with marketing. If a DOOH unit is used for both security and for marketing, or if security information is used for marketing, the notice (and privacy policy) should clearly disclose this.

---

[23]Bill Gerpa, Digital signage networks must guarantee viewer privacy, The Digital Signage Insider, August 1, 2008, http://www.wirespring.com/dynamic_digital_signage_and_interactive_kiosks_journal/articles/Digital_signage_networks_must_guarantee_viewer_privacy-569.html.

[24]Digital Signage Expo, Question of the month, September, 2009, http://www.digitalsignageexpo.net/Resources/QuestionoftheMonth/September09.aspx

[25]TruMedia: Facial Recognition Boards Will Never Record, Share Data, MediaBuyerPlanner, June 11, 2008, http://www.mediabuyerplanner.com/entry/34111/trumedia-facial-recognition-boards-willnever-record-share-data.

[26]The Digital Signage Federation, an industry group, has published a FIPs-based set of privacy guidelines for industry members. *See* Digital Signage Federation, Digital Signage Privacy Standards, February 2011, http://www.digitalsignagefederation.org/Resources/Documents/Articles%20and%20Whitepapers/DSF%20Digital%20Signage%20Privacy%20Standards%2002-2011%20(3).pdf.

CDT conceptualizes three tiers of notice. At minimum, DOOH companies could be required to adopt a symbol to place on signage units, such as on a small placard or appearing on the screen alongside content. The symbol should identify the unit as one that collects some form of consumer data. This approach works best if the symbol is adopted on an industry-wide basis and tested to ensure real consumers understand what it means. If DOOH units include only symbols as notice, a comprehensive notice should also be placed elsewhere in the establishment.

The second tier of notice that could be placed on the DOOH unit would identify the company who owns or operates the unit, inform consumers of what information is being collected. Again, there should be a comprehensive notice elsewhere in the establishment. The third tier is a comprehensive notice that includes the above information, and also the purposes for which the information is being used, with whom the information is shared, what other consumer data will be combined with the information and, if applicable, the choices consumers have with respect to the information being collected.

In cases where DOOH units interact with consumers' devices, such as with smart phones via Bluetooth, a comprehensive notice should also be delivered directly to the consumers' devices. This should be the norm when the DOOH unit or the consumer initiates the interaction.

Internet of Things

The "Internet of Things" is a term used to describe a computerized network of physical objects.[27] The network would be supported by an array of sensors and data storage devices embedded in objects, interacting with web services.[28] The first generation Internet of Things is being built on RFID tags and readers, and the related Near Field Communication, but may also use Bluetooth and other technologies that enable communication at a distance. Because these technologies reveal unique numbers or addresses to readers, they are easily associated with the owners of the tagged objects. Widely deployed, this system would reveal vast amounts of data related to the tagged objects, including location information, environmental conditions and proximity to other objects. Marketers, government or researchers could gather highly detailed data regarding an individual's activities, preferences and habits anywhere the individual goes, not just when an individual is in front of a digital sign.[29]

---

[27] For a detailed discussion, see Int'l Telecomm. Union, ITU Internet Reports 2005: The Internet of Things (7th ed. 2005).

[28] One commonly referenced Internet of Things scenario envisions a refrigerator that can monitor the food it stores. The refrigerator could notify the owner when food spoils, download recipes from websites that make use of the food in the fridge, notify the owner of recalls from the manufacturer, or notify the owner of sales of food he or she prefers. Several early versions of this appliance are out on the market. See Richard MacManus, Internet Fridges: State of the Market, ReadWriteWeb, July 28, 2009 http://www.readwriteweb.com/archives/internet_fridges.php.

[29] As example of an early pervasive tracking system, see the 2008 Cityware research project. Researchers monitored the Bluetooth signals of hundreds of thousands of people without their knowledge in the UK town of Bath. The researchers installed Bluetooth signal receivers in pubs, offices and other public spaces and recorded the collected information in a central database to study how people move in the city. See Paul Lewis, Bluetooth is watching: secret study gives Bath a flavour of Big Brother, The Guardian, July 21, 2008, http://www.guardian.co.uk/uk/2008/jul/21/civilliberties.privacy.

The Internet of Things can bring numerous benefits, but unless careful attention is paid to privacy as the system is being built, the Internet of Things can also create a society in which few moments in our lives go unmonitored or unrecorded. Building the Internet of Things in a manner that preserves its great potential as well as individual privacy will take much work on the part of all the stakeholders in the Internet of Things, including the FTC and a strong commitment to the Fair Information Practice principles, including but certainly not limited to the principle of transparency.

> **What research or other information regarding the effectiveness of disclosures – and, in particular, online disclosures – should the staff consider in revising "Dot Com Disclosures"?**

Researchers have definitively shown that privacy policies do not adequately educate consumers about the ways that their data is collected and used as part of the online advertising ecosystem.

A 2009 study conducted by researchers at UC Berkeley and the University of Pennsylvania's Annenberg School of Communication found that sixty-two percent of respondents incorrectly believe that "If a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission.

Given the considerable length and complexity of most privacy policies, it is no surprise that consumers do not understand their purpose. Researchers at CMU have shown that for a consumer to reach a basic understanding of how his or her information is being collected and used, he or she would have to spend between 181 and 304 hours each year reading Web site privacy policies. Nationally, this sums to between 39.9 and 67.1 billion hours per year spent reading privacy policies, for an estimated annual national economic cost of between 559 billion and 1.1 trillion dollars.[30] In short, while privacy policies can promote accountability, they are not substitutes for simpler consumer disclosures.

> **What issues relating to disclosures have arisen from such multi-party selling arrangements in Internet commerce as (1) established online sellers providing a platform for other firms to market and sell their products online, (2) website operators being compensated for referring consumers to other Internet sites that offer products and services, and (3) other affiliate marketing arrangements?**

In recent years, there has been increasing attention given to the issue of online subscription upselling, the practice of marketing subscription offers to consumers while they are engaged in other separate ecommerce transactions. For example, a consumer purchasing a book from an online vendor might see an offer for an unrelated "shoppers' club membership" from an unknown third party while completing the first transaction. Some first-party vendors and third-party subscription upsellers have employed practices that created misunderstandings and consumer complaints as they presented additional offers to consumers engaged in purchasing goods and services. There has also been concern that some vendors and upsellers have not presented consumers with clear and effective means to obtain refunds and discontinue

[30] Aleecia McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, I/S: A Journal of Law and Policy for the Information Society (2008 Privacy Year in Review issue), *available at* http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.

subscription services. The Senate Commerce Committee and several state Attorneys General have launched investigations into some of these practices.

Online subscription upselling is a relatively new practice without clear standards and guidelines for companies to follow in presenting consumers with subscription upselling offers in a clear, consistent, and fair fashion. Companies should be able to advertise and offer add-on services to consumers engaged in ecommerce transactions, as a consumer may judge that the additional promoted service is worth the advertised price. This can be true for services offered directly by the first-party vendor as well as for a new third-party seller who advertises on the first-party website. Because of the increased chance of confusion due to multiple offers, subscription upsellers — and any first-party vendors that work with subscription upsellers — should abide by a set of best practices to present consumers with legitimate, readily understood offers and meaningful consumer protections.

CDT has led a working group consisting of consumer advocates such as the National Consumers League and industry representatives such as Intelius that together created a set of "best practices" for companies that engage in online subscription upselling. The draft guidelines produced by the working group presently contain recommendations in three general areas: marketing, financial data transfer, and service of upsold subscriptions.[31] Among other "best practices," the draft guidelines recommend that a refund process be offered on all "upsold" subscriptions, giving consumers 60 days to obtain full refunds if they complain they didn't knowingly sign up for the service. Another recommendation is that, for "upsold" subscriptions that convert automatically from free to paid, the subscription upseller should send a confirming email to the consumer before the first charge is billed at the end of the free trial period.

CDT recommends that the Commission look closely at practices related to subscription upselling and craft clear guidance for companies.

Conclusion

The Commission's updated Dot Com Disclosures should reflect an appreciation of businesses' new role as data collectors and of the need for transparency to consumers around this role. Fundamentally, CDT believes that advertisements (and similar business practices) can be deceptive not only in the messages they convey but also in the types of information they surreptitiously collect as they display these messages. We urge the FTC to address this issue in its updated guidelines.

###

About the Center for Democracy & Technology // www.cdt.org

The Center for Democracy & Technology is a non-profit public interest organization working to keep the Internet open, innovative, and free. With expertise in law, technology, and policy, CDT seeks practical solutions to enhance free expression and privacy in communications

[31] Center for Democracy & Technology, *Online Subscription Upselling Working Group, Best Practices Working Draft* (2010), http://www.cdt.org/files/pdfs/20102113_upselling_best_practices.pdf.

technologies. CDT is dedicated to building consensus among all parties interested in the future of the Internet and other new communications media.

For further information, please contact:

Justin Brookman
Director, Consumer Privacy Project
+1 202-637-9800
justin@cdt.org

Erica Newland
Policy Analyst
+1 202-637-9800
erica@cdt.org